**Literature Review on Fairness of Smart Contracts**

**All Papers Introductions:**

1. **FairSwap: How to Fairly Exchange Digital Goods**

* **Main Point**: FairSwap introduces a smart contract protocol to ensure fairness in digital exchanges, minimizing blockchain costs and enhancing security by using efficient cryptographic hash functions and commitment schemes rather than costly zero-knowledge proofs.

1. **Blockchain Smart Contracts: Applications, Challenges, and Future Trends**

* **Main Point**: This paper provides a comprehensive review of smart contract technologies, emphasizing the challenges in ensuring fair execution due to issues like immutability, reliance on oracles, scalability, and performance.

1. **Distributed Proportional-Fairness Control in MicroGrids via Blockchain Smart Contracts**

* **Main Point**: This paper presents a proportional-fairness control strategy for distributed energy resources in microgrids, using blockchain smart contracts to ensure fair rotation and equitable distribution of responsibilities among participants.

1. **ZEUS: Analyzing Safety of Smart Contracts**

* **Main Point**: ZEUS offers a framework for verifying the correctness and fairness of smart contracts through abstract interpretation and symbolic model checking, ensuring contracts follow intended business logic and preventing unfair advantages.

1. **Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law**

* **Main Point**: Levy critiques the social limitations of smart contracts, highlighting how their rigid enforcement mechanisms fail to account for the nuanced social functions of traditional contracts, such as behavioral expectations and flexible terms.

1. **Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts**

* **Main Point**: Ekiden integrates Trusted Execution Environments (TEEs) with blockchain to enhance the confidentiality, performance, and security of smart contracts, addressing fairness issues by preventing data exposure and improving throughput.

1. **Fair Hierarchical Secret Sharing Scheme Based on Smart Contract**

* **Main Point**: This paper proposes a blockchain-based hierarchical threshold secret sharing scheme, ensuring fairness by penalizing dishonest behavior through financial deposits and using smart contracts for secure and efficient secret reconstruction.

1. **Smart Contract for Multiparty Fair Certified Notifications**

* **Main Point**: This paper introduces a blockchain-based protocol for certified notifications, ensuring fairness by guaranteeing either all parties receive the expected items or none do, reducing reliance on intermediaries and maintaining transparency.

1. **A Fair and Trusted Trading Scheme for Medical Data Based on Smart Contracts**

* **Main Point**: This paper proposes a smart contract-based system using zero-knowledge proofs and a Stackelberg game model to ensure fairness in medical data transactions, balancing privacy protection with equitable pricing.

1. **Quantised and Simulated Max–min Fairness in Blockchain Ecosystems**

* **Main Point**: This study explores fairness in resource allocation within blockchain ecosystems through Max-min Fairness algorithms, ensuring equitable distribution while addressing scalability and complexity challenges.

**Paper [1]:**

FairSwap: How to fairly exchange digital goods

**Introduction**

Fairness in smart contracts is pivotal for ensuring trust and equity in digital transactions. The concept encompasses guaranteeing that all parties involved receive what they are owed without the need for intermediaries, thus mitigating risks of fraud and disputes. FairSwap, as introduced by Dziembowski, Eckey, and Faust, provides a significant advancement in the realm of fair exchange of digital goods by utilizing smart contracts over decentralized cryptocurrencies, primarily focusing on minimizing costs and enhancing security.

**Critical Analysis**

The paper "FairSwap: How to Fairly Exchange Digital Goods" proposes a protocol that addresses the fairness problem in digital exchanges using smart contracts. Traditional approaches often require a trusted third party or are burdened with high computational costs, especially for large digital goods. FairSwap circumvents these issues by employing a smart contract to act as an external judge, ensuring that the receiver only pays if the digital good received is correct, and the sender receives payment upon correct delivery.

Key elements of FairSwap include:

1. **Cost Efficiency**: The protocol minimizes blockchain execution costs by avoiding expensive cryptographic tools such as zero-knowledge proofs, instead relying on efficient cryptographic hash functions and commitment schemes.
2. **Proof of Misbehavior**: This innovative concept allows the protocol to efficiently handle disputes by enabling the receiver to prove the sender’s misbehavior if the delivered digital good is incorrect, thereby safeguarding fairness.
3. **Scalability**: The protocol is particularly effective for large digital commodities, providing a scalable solution that reduces the data processed by the smart contract to a manageable size, thus lowering transaction fees.

**Comparison with Existing Literature**

Previous works on fair exchange protocols, such as those utilizing zero-knowledge contingent payments (ZKCP), often encounter high computational overheads and inefficiencies when dealing with complex or large transactions. FairSwap, however, integrates the benefits of low-cost smart contracts with minimal computational burden on users, setting it apart from other solutions. Additionally, while traditional escrow services or centralized trusted parties can be unreliable or costly, FairSwap leverages decentralized cryptocurrencies to replace these intermediaries, providing a more secure and economical alternative.

**Gaps and Limitations**

Despite its advantages, FairSwap’s reliance on the underlying blockchain’s consensus mechanism introduces a dependency on the network's security and efficiency. Any vulnerabilities or inefficiencies in the blockchain could potentially affect the fairness and execution of the protocol. Moreover, the protocol assumes honest behavior from participants until proven otherwise, which, while mitigated by the proof of misbehavior, does not eliminate the risk of malicious attempts to game the system.

**Conclusion**

FairSwap significantly advances the fairness in digital exchanges using smart contracts, offering a cost-effective, scalable, and secure solution. By addressing the limitations of previous protocols and integrating innovative mechanisms for dispute resolution, it sets a new standard for fair digital transactions. Further research could focus on enhancing the robustness of such protocols against blockchain vulnerabilities and exploring their applications in more diverse transaction types.

**Paper [2]:**

Blockchain smart contracts: Applications, challenges, and future trends

**Introduction**

Fairness in smart contracts is a critical aspect ensuring that all parties involved in a transaction are treated equitably and their agreements are enforced without bias. This concept is essential for fostering trust and reliability in decentralized systems. Smart contracts are designed to automate and enforce agreements using blockchain technology, removing the need for intermediaries and ensuring transparency. This review synthesizes the insights from the attached research paper and other relevant literature on the fairness of smart contracts, focusing on the technical and practical aspects.

**Critical Analysis**

The paper "Blockchain smart contracts: Applications, challenges, and future trends" by Khan et al. provides an extensive survey of smart contract technologies, highlighting several fairness-related concerns. One primary focus is on the inherent challenges in ensuring fair execution of contracts, especially concerning the immutability and consensus mechanisms. The authors discuss how immutability, while a strength for security, poses fairness issues when errors or fraud occur since contracts cannot be easily modified or terminated.

The paper also addresses the reliance on off-chain resources through oracles, which can introduce biases or errors if the oracle data is incorrect. This reliance challenges the fairness of the smart contract execution, as it depends heavily on the accuracy and trustworthiness of the external data source.

Another significant point is the issue of scalability and performance, which indirectly affects fairness. In a congested network, transactions may be delayed or incur high fees, disadvantaging users with fewer resources. The study compares different blockchain platforms like Ethereum and Hyperledger Fabric, noting that while some offer better scalability or security features, none perfectly address all fairness concerns.

**Summary and Comparison with Other Literature**

The key points regarding fairness from the paper include:

1. **Immutability and Flexibility**: While immutability ensures security, it limits the ability to rectify errors, impacting fairness when changes are necessary.
2. **Oracles and Off-Chain Data**: Dependence on external data sources could compromise fairness if the data provided is inaccurate or biased.
3. **Scalability and Costs**: Network congestion and high transaction fees can lead to inequitable access and processing times.

These findings align with other literature in the field, which also highlights these issues as significant barriers to achieving complete fairness in smart contracts. For instance, FairSwap and other protocols attempt to address fairness in specific contexts but often face similar limitations regarding off-chain data and transaction costs.

**Gaps and Limitations**

The paper identifies several gaps in current research, such as the need for improved consensus mechanisms that balance security, scalability, and fairness. It also points out the lack of standardized frameworks for evaluating the fairness of smart contracts, suggesting that future research should focus on developing comprehensive metrics and tools for this purpose.

**Conclusion**

Ensuring fairness in smart contracts remains a complex challenge due to technical limitations and the reliance on external data. While current solutions offer partial mitigation, comprehensive frameworks and improved technologies are required to address these issues fully. The findings from Khan et al. provide a valuable foundation for future research aimed at enhancing the fairness and reliability of smart contract systems.

**Paper [3]:**

Distributed Proportional-Fairness Control in MicroGrids via Blockchain Smart Contracts

**Introduction**

Fairness in smart contracts is crucial for ensuring equitable outcomes for all parties involved, particularly in decentralized systems like blockchain networks. The concept involves the unbiased enforcement of agreements, trustless transactions, and balanced resource allocation. The paper "Distributed Proportional-Fairness Control in MicroGrids via Blockchain Smart Contracts" by Danzi et al. explores these aspects in the context of managing Distributed Energy Resources (DERs) in microgrids.

**Critical Analysis**

The study introduces a proportional-fairness control strategy for DERs to mitigate the issue of power surplus and voltage instability in residential microgrids. The fairness aspect is achieved by dynamically selecting subsets of DERs to curtail their power output based on their historical participation in voltage regulation. This approach ensures that no single DER consistently bears the burden of curtailment, promoting an equitable distribution of responsibilities.

Key points regarding fairness in the paper include:

1. **Proportional Fairness Mechanism**: DERs that frequently contribute to voltage regulation are less likely to be selected in subsequent periods, ensuring a fair rotation among all DERs.
2. **Credit-Based Incentive System**: DERs receive credits for participating in voltage regulation, which they can use to avoid curtailment in future periods, balancing the economic impact across participants.
3. **Decentralized Control via Blockchain**: The use of blockchain ensures trust and transparency in the system by recording all transactions and credit histories, eliminating the need for a central authority.

Comparatively, other literature on smart contracts often highlights issues such as the immutability of contracts and dependency on off-chain data, which can affect fairness. Danzi et al. address these by using a decentralized blockchain protocol that maintains a tamper-proof record of DER activities and credit statuses, reducing the risk of unfair manipulation.

**Gaps and Limitations**

The paper identifies several limitations in the proposed system:

1. **Dependency on Blockchain Efficiency**: The effectiveness of the proposed solution relies on the efficiency of the blockchain network. High computational costs and potential delays in block generation could impact the timely execution of the smart contracts.
2. **Uniform Hardware Assumption**: The security of the system assumes uniform computational power across DERs, which might not be realistic in all scenarios.
3. **Communication Overhead**: The decentralized nature of the blockchain introduces higher communication costs compared to centralized systems, which might limit scalability.

**Conclusion**

The study by Danzi et al. provides a robust framework for achieving fairness in the control of DERs in microgrids through blockchain-based smart contracts. By ensuring equitable participation and using a transparent credit-based incentive system, the proposed solution addresses many fairness concerns prevalent in decentralized energy systems. However, the reliance on blockchain efficiency and the associated communication costs highlight areas for further research and optimization.

**Paper [4]: [Important]**

ZEUS: Analyzing Safety of Smart Contracts

#### **Introduction**

Fairness in smart contracts is essential for ensuring equitable outcomes and trust among all parties involved in decentralized transactions. The concept involves the fair execution of agreements, adherence to agreed-upon rules, and unbiased treatment of participants. This literature review synthesizes insights from the paper "ZEUS: Analyzing Safety of Smart Contracts" by Kalra et al., along with other relevant literature, focusing on fairness issues and mechanisms within smart contracts.

#### **Critical Analysis**

The paper "ZEUS: Analyzing Safety of Smart Contracts" highlights the importance of both correctness and fairness in smart contracts. Fairness is defined as adherence to higher-level business logic, ensuring that the smart contract's behavior aligns with the agreed-upon rules and expectations of all participants. ZEUS is a framework designed to verify the correctness and validate the fairness of smart contracts by leveraging abstract interpretation and symbolic model checking.

Key points regarding fairness from the paper include:

1. **Fairness Validation**: ZEUS ensures that smart contracts follow the intended business logic, preventing any party from gaining unfair advantages. This is critical in scenarios where financial transactions and multi-party agreements are involved.
2. **Automated Verification**: By automating the verification process, ZEUS reduces human error and ensures a more reliable validation of both correctness and fairness, addressing issues that might be overlooked in manual audits.
3. **Handling Reentrancy and State Dependence**: The framework identifies and mitigates common fairness issues such as reentrancy attacks and state dependence, which can lead to unfair outcomes if not properly managed.

In comparison with other literature, ZEUS stands out due to its comprehensive approach to automated verification. While other tools like Oyente focus on security vulnerabilities, ZEUS integrates fairness checks into its analysis, making it more holistic.

#### **Summary and Comparison with Other Literature**

The key contributions of ZEUS regarding fairness include:

* **Abstract Interpretation and Symbolic Model Checking**: These techniques allow for a thorough analysis of smart contracts, ensuring that they adhere to both safety and fairness criteria.
* **Zero False Negatives**: ZEUS claims a high accuracy in detecting fairness issues, with a low false positive rate, which is a significant improvement over previous tool.

Other studies in the field often highlight the challenges of ensuring fairness due to the immutable nature of smart contracts and the complexity of multi-party interactions. ZEUS addresses these challenges by providing a robust framework for pre-deployment verification, reducing the risk of unfair practices once the contract is live.

#### **Gaps and Limitations**

Despite its strengths, the paper identifies several limitations in the ZEUS framework:

1. **Complexity in Policy Specification**: Defining fairness policies can be complex and requires careful consideration of all possible contract states and interactions.
2. **Performance Overhead**: The verification process, although efficient, introduces some performance overhead, which might be a concern for very large or highly complex contracts.
3. **Generalizability**: While ZEUS supports Ethereum and Fabric, its applicability to other blockchain platforms and smart contract languages may require additional adaptation and validation.

#### **Conclusion**

ZEUS significantly advances the state of the art in ensuring fairness in smart contracts through automated verification. By addressing both correctness and fairness, it provides a comprehensive solution to the challenges of deploying reliable and equitable smart contracts. Future research should focus on extending the framework's applicability and further refining its performance to handle increasingly complex smart contract scenarios.

**Paper [5]:**

Book-Smart, Not Street-Smart:

Blockchain-Based Smart Contracts and The Social Workings of Law

**Introduction:**

The concept of fairness in smart contracts involves ensuring that automated and secure digital agreements, executed via blockchain technology, uphold equitable and just outcomes for all parties involved. Smart contracts promise efficiency and precision by removing intermediaries and reducing enforcement costs. However, the social dimensions of fairness, such as the adaptability and relational context within which traditional contracts operate, present challenges for these technologically driven agreements.

**Critical Analysis:**

Karen E. C. Levy's paper, "Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law," provides a critical examination of smart contracts, highlighting their inherent limitations in addressing fairness. Levy argues that smart contracts, while technically robust, often neglect the nuanced social functions of traditional contracts, such as the inclusion of unenforceable terms to set behavioral expectations, vague terms to foster long-term relationships, and strategic nonenforcement as a bargaining tool.

**Summary of Main Points:** Levy identifies three key areas where smart contracts fall short of achieving fairness:

1. **Unenforceable Terms:** Traditional contracts often include terms that are legally unenforceable but serve to communicate expectations and influence behavior. Smart contracts' rigid enforcement mechanisms fail to account for this social utility.
2. **Vague Terms:** Vague terms in traditional contracts allow for flexibility and adaptation over time, supporting long-term relationships. Smart contracts' requirement for precise terms can undermine these relational benefits.
3. **Strategic Nonenforcement:** The possibility of choosing not to enforce certain terms strategically fosters negotiation and relational harmony. The automatic enforcement of smart contracts does not accommodate this social practice.

**Gaps, Contradictions, and Limitations:**

Levy critiques the oversimplification of legal processes in smart contracts, pointing out that they are designed with a narrow view of contractual functions, focused on technical efficiency over social dynamics. This inflexibility can disadvantage parties who rely on the social aspects of traditional contracts to manage relationships and expectations. The paper suggests that while smart contracts can reduce transaction costs, they might also exacerbate inequalities by failing to consider the socio-economic barriers to justice.

**Conclusion:**

Smart contracts hold the potential for transforming contract enforcement by leveraging blockchain technology. However, to achieve true fairness, it is essential to integrate the social and relational contexts within which contracts operate. Levy's analysis underscores the need for a more comprehensive understanding of how law functions socially, advocating for the inclusion of these considerations in the development and deployment of smart contracts.

**Paper [6]:**

Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts

**Introduction**

Fairness in smart contracts encompasses the equitable execution and enforcement of agreements among distrusting parties on a blockchain. It ensures that no party can alter or unfairly influence the contract's terms or execution. As blockchain technologies evolve, the challenge of maintaining fairness, particularly concerning performance, confidentiality, and availability, becomes more pronounced. This literature review examines these aspects as highlighted in the research on Ekiden, a platform designed to address critical gaps in current smart contract implementations.

**Critical Analysis**

The paper "Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts" presents a novel system combining Trusted Execution Environments (TEEs) and blockchains to enhance fairness in smart contracts. The integration of TEEs aims to resolve confidentiality issues while maintaining high performance and security. The authors systematically identify and address the pitfalls of harmonizing TEEs with blockchains, such as the risk of block forgery and timing attacks, which are crucial for ensuring fairness.

Key points regarding fairness include:

1. **Confidentiality**: Ekiden ensures that contract data remains confidential, preventing any party from gaining an unfair advantage through data exposure.
2. **Performance**: By offloading computations to TEEs, Ekiden significantly improves the throughput and reduces latency, promoting fairness by enabling more complex and responsive smart contracts.
3. **Security**: The system's design mitigates potential attacks that could compromise fairness, such as integrity attacks on the blockchain that could lead to unauthorized state manipulations.

Despite these advancements, the paper acknowledges several limitations. The dependency on TEEs introduces new attack vectors, and the system's effectiveness hinges on the assumption that TEEs remain uncompromised. Additionally, while Ekiden addresses many fairness issues inherent in current blockchain systems, it still relies on the underlying blockchain's consensus mechanism, which may not be entirely fair in all scenarios.

Compared to other literature, Ekiden's approach to combining TEEs and blockchain offers a robust solution to fairness but highlights the need for continuous monitoring and improvement of TEE technologies. Other studies, such as those exploring zero-knowledge proofs and secure multiparty computation, offer alternative methods to achieve fairness but often at the cost of performance and scalability.

In conclusion, Ekiden represents a significant step towards fairer smart contracts by leveraging the complementary strengths of TEEs and blockchains. However, it also underscores the ongoing challenges and the need for multi-faceted approaches to fully realize fair and equitable smart contract systems.

**Paper [7]:**

Fair hierarchical secret sharing scheme based on smart contract

**Introduction**

Fairness in smart contracts is pivotal for ensuring that all participants in a transaction or agreement receive equitable treatment without the reliance on trusted third parties. Smart contracts, powered by blockchain technology, provide an automated, decentralized mechanism to enforce agreements. In the context of secret sharing schemes, fairness implies that all participants either obtain the secret simultaneously or none do, preventing any single party from gaining an undue advantage.

**Summary and Critical Analysis**

This paper introduces a fair hierarchical threshold secret sharing (HTSS) scheme based on blockchain, leveraging smart contracts to ensure fairness. The authors address the inherent inefficiencies and fairness issues in traditional secret sharing schemes, which often rely on trusted third parties or require multiple communication rounds. Their proposed scheme ensures that all participants commit to their secret shares via a smart contract, which penalizes dishonest behavior through financial deposits. This innovative approach guarantees that participants either reveal their shares within a specified timeframe or incur a penalty, thus maintaining fairness without a central authority.

The integration of Birkhoff interpolation allows for the reconstruction of the secret in a single round, enhancing efficiency and reducing computational overhead. The scheme's security is formally proven, and its practical implementation on the Ethereum test network demonstrates its feasibility and performance efficiency.

**Gaps and Limitations**

While the proposed scheme significantly advances the state of fairness in secret sharing, it assumes that the deposit value is always higher than the value of the secret, which might not be practical in all scenarios. Furthermore, the reliance on Ethereum's gas fees for transactions could pose economic constraints for large-scale implementations. Future research could explore adaptive deposit mechanisms and scalability solutions to address these limitations.

**Conclusion**

This research papers contribution to fair secret sharing using smart contracts marks a significant step towards decentralized and efficient secret reconstruction. By addressing the shortcomings of previous schemes, this approach provides a robust framework for fair and secure multiparty computations.

**Paper [8]:**

Smart Contract for Multiparty Fair Certified Notifications

**Introduction**

The concept of fairness in smart contracts is critical to ensuring equitable and trustworthy transactions between parties. Fairness is particularly important in the context of certified notifications, where proof of message origin and receipt is exchanged. This literature review focuses on the fairness aspects of smart contracts, synthesizing insights from the paper "Smart Contract for Multiparty Fair Certified Notifications" by Payeras-Capellà and comparing these findings with existing literature.

**Critical Analysis**

This paper introduced a blockchain-based protocol for multiparty fair certified notifications, emphasizing confidentiality, fairness, and timeliness with minimal reliance on a stateless Trusted Third Party (TTP). The paper argues that traditional fair exchange protocols heavily depend on TTPs to resolve conflicts, which blockchain technology and smart contracts can mitigate by providing a decentralized and verifiable solution.

The proposed protocol ensures fairness by guaranteeing that either all parties receive the expected items or none do. This approach aligns with the principle of fair exchange where no party is disadvantaged. The use of blockchain and smart contracts reduces the need for TTPs, thus decreasing transaction costs and delays while maintaining transparency and security.

**Main Points on Fairness**

1. **Fair Exchange**: The protocol ensures that either each party receives the expected item or none do, minimizing the risk of unfair advantage.
2. **Optimistic Protocol**: The system operates optimistically, meaning it can complete transactions without TTP intervention unless a dispute arises.
3. **Stateless TTP**: When TTP involvement is necessary, it does not store exchange states, leveraging the blockchain for public verification.
4. **Timeliness**: The protocol allows parties to unilaterally terminate transactions without compromising fairness, ensuring prompt resolution.
5. **Non-repudiation**: It ensures that neither the sender nor the receiver can deny the exchange, which is crucial for accountability and trust.

**Comparative Analysis**

Compared to traditional protocols that rely on TTPs, the blockchain-based approach offers significant improvements in reducing reliance on intermediaries. Studies like Liu et al. (2017) [11] and Barber et al. (2012) [12] highlight the potential of smart contracts in achieving fairness without TTPs, supporting the findings of Payeras-Capellà et al. However, the paper identifies that while the protocol achieves weak fairness, it does not fully address the transferability of proofs, which is a noted limitation.

**Conclusion**

The integration of blockchain technology in smart contracts for certified notifications enhances fairness by ensuring equitable exchanges, reducing dependency on intermediaries, and maintaining transparency. Despite some limitations, such as the non-transferability of proofs, the proposed protocol represents a significant advancement in achieving fairness in multiparty exchanges, aligning with broader trends in blockchain research. Further studies could focus on enhancing proof transferability to address this gap.

**Paper [9]:**

**A Fair and Trusted Trading Scheme for Medical Data Based on Smart Contracts**

**Introduction**

The concept of fairness in smart contracts is pivotal in ensuring equitable and transparent digital transactions, particularly in sensitive sectors like healthcare. Fairness in this context refers to the assurance that all parties involved in a transaction are treated justly, their data is securely handled, and they receive appropriate incentives for their participation. The literature extensively discusses fairness mechanisms in smart contracts, focusing on enhancing trust, data authenticity, and equitable pricing strategies.

**Critical Analysis**

The paper "A Fair and Trusted Trading Scheme for Medical Data Based on Smart Contracts" by Yang and Zhang presents a comprehensive approach to ensuring fairness in medical data transactions. The authors propose a smart contract-based system that leverages zero-knowledge proofs for data verification and a Stackelberg game model for fair pricing​​. This dual approach addresses both the authenticity of medical data and the equitable distribution of transaction benefits.

The use of zero-knowledge proofs ensures that data authenticity can be verified without exposing sensitive information, thus maintaining privacy while building trust among participants​​. This method effectively creates a solid privacy protection barrier before transactions, which is critical in healthcare data management​​.

The study highlights key points regarding fairness:

1. **Zero-Knowledge Proofs**: Ensuring data authenticity while protecting privacy, fostering trust among participants.
2. **Game Pricing Strategy**: Implementing a Stackelberg game model to balance incentives and achieve equitable pricing.
3. **Blockchain Integration**: Utilizing blockchain for tamper-proof record-keeping, enhancing transparency and trust.

Despite its strengths, the study reveals certain gaps and limitations. For instance, while the zero-knowledge proof mechanism effectively addresses privacy concerns, the computational overhead and complexity may pose challenges for large-scale adoption. Moreover, the reliance on blockchain technology, although beneficial for security, may encounter scalability issues, particularly in handling high transaction volumes.

Furthermore, the application of the Stackelberg game model in pricing strategies aims to achieve a Nash equilibrium, ensuring that both data providers and consumers maximize their benefits. This game-theoretic approach not only enhances fairness in pricing but also incentivizes participation by ensuring reasonable returns for all parties involved​​.

Compared to other frameworks, this scheme uniquely combines privacy protection with fair transaction incentives, setting it apart from traditional centralized systems which often suffer from opacity and potential dishonesty​​. However, the paper also identifies gaps in the current research, particularly the challenge of integrating such decentralized systems with existing hospital infrastructures and the potential delays in transaction processing due to blockchain’s consensus mechanisms​​.

**Conclusion**

Yang and Zhang's framework for fair and trusted medical data transactions via smart contracts represents a significant advancement in addressing fairness. By integrating zero-knowledge proofs and the Stackelberg game model, the proposed scheme ensures data authenticity, privacy, and equitable pricing, thus encouraging broader participation and trust in digital health ecosystems. Future research should focus on optimizing blockchain performance and seamless integration with existing systems to fully realize the potential of these innovative fairness mechanisms in smart contracts.

**Paper [10]:**

**Quantised and Simulated Max–min Fairness in Blockchain Ecosystems**

**Introduction**

Fairness in smart contracts is crucial for ensuring user participation and trust in blockchain ecosystems. The concept revolves around the equitable distribution of resources and transparency in operations, which are fundamental to maintaining the integrity and efficiency of these systems. This review synthesizes insights from the attached paper "Quantised and Simulated Max–min Fairness in Blockchain Ecosystems" by Serdar Metin and Can Özturan, as well as relevant literature on the topic.

**Main Points on Fairness**

The paper explores fairness through the implementation of Max-min Fairness (MF) algorithms in blockchain ecosystems, specifically focusing on resource allocation via blockchain faucets. It introduces four decentralized algorithms: Quantised Max-min Fairness (QMF), Simulated Max-min Fairness (SMF), and their weighted versions. These algorithms aim to ensure fair distribution of resources by adapting MF, a well-established fair distribution scheme in computer science, to the constraints of blockchain systems.

1. **Quantised Max-min Fairness (QMF)**: This algorithm limits the demand volume but scales to many users. It ensures fairness by allocating resources based on predefined intervals.
2. **Simulated Max-min Fairness (SMF)**: This algorithm restricts the number of users but allows for various weighting policies. It is designed to handle different user demands dynamically.
3. **Weighted Versions**: The weighted versions of QMF and SMF introduce user-specific weights, enhancing the flexibility and fairness of the resource distribution process.

**Critical Analysis**

The study by Metin and Özturan provides a significant contribution to the field by addressing the fairness of resource distribution in non-commercial blockchain networks. However, it highlights some limitations:

* **Scalability**: While QMF scales well with user numbers, SMF is limited by the number of users it can efficiently support due to computational constraints.
* **Complexity**: The implementation of weighted versions increases the complexity, which may impact the performance and ease of adoption in various blockchain environments.
* **Demand Constraints**: QMF's restriction on demand volumes may not cater to all use cases, limiting its applicability in scenarios with highly variable resource requirements.

**Comparison with Other Literature**

Compared to other studies, such as those focusing on fair distribution in cloud or IoT environments, this paper uniquely addresses the intricacies of blockchain ecosystems. Other works often assume centralized control mechanisms or different economic models, whereas Metin and Özturan's approach is decentralized and tailored for non-commercial settings, filling a gap in the literature on blockchain-based fairness.

**Conclusion**

The study effectively adapts traditional fairness algorithms to the blockchain context, providing robust solutions for fair resource distribution. Despite certain limitations, the proposed algorithms enhance the understanding and implementation of fairness in smart contracts, offering valuable frameworks for future research and development in this area.

**References:**

1. Dziembowski, S., Eckey, L., & Faust, S. (2018, October). Fairswap: How to fairly exchange digital goods. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 967-984).
2. Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-peer Networking and Applications*, *14*, 2901-2925.
3. Danzi, P., Angjelichinoski, M., Stefanović, Č., & Popovski, P. (2017, October). Distributed proportional-fairness control in microgrids via blockchain smart contracts. In *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)* (pp. 45-51). IEEE
4. Kalra, S., Goel, S., Dhawan, M., & Sharma, S. (2018, February). Zeus: analyzing safety of smart contracts. In *Ndss* (pp. 1-12)
5. Levy, K. E. (2017). Book-smart, not street-smart: blockchain-based smart contracts and the social workings of law. *Engaging Science, Technology, and Society*, *3*, 1-15
6. Cheng, R., Zhang, F., Kos, J., He, W., Hynes, N., Johnson, N., ... & Song, D. (2019, June). Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 185-200). IEEE
7. Zhang, E., Li, M., Yiu, S. M., Du, J., Zhu, J. Z., & Jin, G. G. (2021). Fair hierarchical secret sharing scheme based on smart contract. *Information Sciences*, *546*, 166-176
8. Payeras-Capellà, M., Mut-Puigserver, M., & Cabot-Nadal, M. À. (2018, November). Smart contract for multiparty fair certified notifications. In *2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW)* (pp. 459-465). IEEE
9. Yang, X., & Zhang, K. (2024). A Fair and Trusted Trading Scheme for Medical Data Based on Smart Contracts. *Computers, Materials & Continua*, *78*(2).
10. Metin, S., & Özturan, C. (2024). Quantised and Simulated Max–min Fairness in Blockchain Ecosystems. *Future Generation Computer Systems*, *151*, 260-271.
11. Liu, J., Li, W., Karame, G. and Asokan, N.: ”Towards Fairness of Cryptocurrency Payments”, IEEE Security and Privacy, 2017.
12. Barber, S., Boyen, X. Shi, E. and Uzun, E., ”Bitter to Better — How to Make Bitcoin a Better Currency”. Financial Cryptography and Data Security, Springer Berlin Heidelberg, p.399-414, 2012.